

UNITED STATES DISTRICT COURT

for the

Middle District of Alabama

RECEIVED

2018 MAY 30 A 10: 50

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Residence & curtilage located at 24988 Harmony
Church Rd, Andalusia, AL 36420, including outbuildings,
vehicles, computers or computer-related storage devices, &
persons assoc. w/ address (See Att's A & B).

Case No. 2:18-mj-00130-WE
DEBRA R. HACKETT, CLK
U.S. DISTRICT COURT
MIDDLE DISTRICT OF ALA

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Middle District of Alabama, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

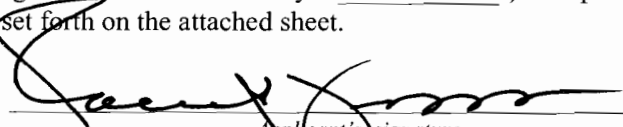
Offense Description

18 U.S.C. §§ 2252 and 2252A Transport, distribute, receive, and/or possess child pornography.

The application is based on these facts:

See Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Robert J. Thompson, SAS/TFO ABI/DHS HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 05/30/2018



Judge's signature

City and state: Montgomery, AL

Wallace Capel, Jr., Chief U.S. Magistrate Judge

Printed name and title

RECEIVED

2018 MAY 30 A 10:50

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA**

RODA B. WICKETT, CLK
U.S. DISTRICT COURT
MIDDLE DISTRICT ALA

In the Matter of the Search of:

The residence and curtilage located at
24988 Harmony Church Road, Andalusia,
Alabama, 36420, including any outbuildings,
vehicles, and computers or computer-related
storage devices, and persons associated with
address as further described in Attachments A
and B.

Case No. 2:18-mj-130-WC

UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT

I, Robert J. Thompson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I, Robert J. Thompson am a Special Agent Senior with the Alabama Bureau of Investigation, Montgomery, Alabama. I graduated from the Alabama State Trooper Academy, and received my certification from the Alabama Peace Officers' Standards and Training Commission. Currently, I am assigned as a Special Agent with the Alabama Law Enforcement Agency and am assigned to the Special Victims Unit, Internet Crimes Against Children Task Force (ICAC) and as a Federal Task Force Officer with US Department of Homeland Security HSI.

2. My duties include the detection and investigation of alleged crimes, including, but not limited to, investigating crimes against children and adults, exploitation of children and child pornography. I have received extensive training in investigative techniques and undercover operations involving computer facilitated exploitation of children. I have also been trained in computer forensics by the USSS National Computer Forensics Institute in Hoover, Alabama, the Internet Crimes against Children (ICAC) Task Force Training and the National White Collar Crime Center. I have conducted investigations of these types of crimes and have assisted other

Purdin-1823000001CE

law enforcement agents with investigations of this nature, and I have written and executed numerous search warrants in the State of Alabama.

3. I am investigating the activities of someone using an Internet Protocol (IP) address registered to Robert and Tracy PURDIN at the following address: 24988 Harmony Church Road, Andalusia, Alabama 36420. As will be shown below, there is probable cause to believe that someone has used that IP address to transport, distribute, receive, and/or possess child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A.

4. I submit this application and affidavit in support of a search warrant authorizing a search of the residence and curtilage located at 24988 Harmony Church Road, Andalusia, Alabama 36420, including any outbuildings, computers, or computer-related storage devices found thereon, as further described in **Attachment A** (the "SUBJECT PREMISES"). I am also seeking authority to seize on and within the SUBJECT PREMISES the items specified in **Attachment B** and subsequently search, which may constitute evidence, fruits, and instrumentalities of the forgoing criminal violations.

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A are present on the SUBJECT PREMISES. This search warrant also asserts probable cause to search the person of any individual present at the SUBJECT PREMISES for any and all items listed in Attachment B.

CRIMINAL STATUTES

6. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

7. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

8. 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed or shipped or transported in interstate or foreign commerce. That section also makes it a federal crime for any person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

9. 18 U.S.C. § 2252(a)(4) prohibits a person from knowingly possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce or that were produced using materials that had traveled in interstate or foreign commerce.

10. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping child pornography using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

11. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

12. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or accessing with intent to view any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped and transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

13. “Child Erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

14. “Child Pornography,” as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

15. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

16. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

17. “Computer,” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such devices.” For purposes of this

search warrant, the term “computer” also encompasses computer software and data security devices.

18. “Computer-related media,” as used herein, encompasses all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data, including any data-processing devices (such as central processing units, internal drives, and fixed disks); peripheral storage devices (such as external hard drives, floppy diskettes, compact discs (CDs), digital video disks (“DVDs”), Personal Digital Assistants (“PDAs”), memory cards, Subscriber Identity Module (“SIM”) cards, and USB thumb drives); peripheral input/output devices (such as modems, routers, keyboards, printers, scanners, copiers, monitors, web cams, digital cameras, iPods, cell phones, and video game consoles); as well as related equipment (such as cables and connectors).

19. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

20. “Data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code

may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

21. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

22. “Minor” means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

23. “Peer-to-peer” or “P2P” file-sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user’s computer, and conducting searches for files that are currently being shared on another user’s computer.

24. The phrase “records, documents, and materials” includes all information recorded in any form by any means, whether in handmade form (such as writings, drawings, or paintings); photographic form (such as developed film, print-outs, slides, negatives, or magazines); type-written form (such as print-outs, books, pamphlets, or other typed documents); audio/visual form (such as tape-recordings, videotapes, DVDs, or CDs); or electronic form (such as digital data files, file properties, computer logs, or computer settings).

COMPUTERS AND CHILD PORNOGRAPHY

25. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the way in which child pornography is produced and distributed.

26. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

27. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

28. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

29. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

30. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography can sometimes be found on the user's computer, and even

when online storage is used, it is still possible to find evidence of child pornography activity on the user's computer.

31. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others.

32. The Internet can be accessed through the use of a router. Routers often store important information about other computers that have obtained Internet access through them. A wireless router is a device that performs the functions of a router without the need for a cabled connection. If an unauthorized user obtains access to the Internet via another person's wireless router, evidence of the unauthorized access can often be found on the router itself.

33. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools.

34. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by

new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed and more on a particular user's operating system, storage capacity, and computer habits.

PEER-TO-PEER (P2P) FILE SHARING

35. Peer-to-Peer (P2P) file sharing computer software programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files. Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

36. I know from my training and experience that P2P file sharing networks are frequently used to trade digital files of child pornography. These files include both image and movie files.

37. During the default installation of most P2P software applications, settings are established which configure the host computer to share files. Depending upon the software application used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, there are settings that allow the user to establish the location of one or more directories or folders whose contents (files) are made available for distribution to other network users and to control (a) whether or not files are made available for distribution to other network users; (b) whether or not other network users can obtain a list of the files being shared by the host computer; and (c) whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

38. There is a feature inherent in all P2P programs that allows for requesting a shared file listing directly from a computer. P2P investigators have received training and have used the features built into the Gnutella P2P Client software programs to request a file listing of "shared files" from various computers during undercover P2P operations. The command used is commonly called a "browse." This command allows the computer host (a host is a term used to describe a computer connected to the Internet) making the request to "browse" or look through a listing of files by name, file type, quality and SHA-1 values that the user on the other end has specifically placed or downloaded into a specific folder for sharing with others on the P2P Network. A browse command is available to any and all users on the Gnutella Network and is part of the commonality in all Gnutella Clients or software. Users can and do share or have files in their shared folder available for searches and downloads on the Gnutella Network. Users can also disallow "browsing" of their shared files. Anyone who routinely uses and downloads files

would know they are downloading from other users who have allowed file sharing on their computer. The sharing concept is the whole concept and reason for a user installing a P2P client or software. Conversely, they would also know that certain files on their computer are available for download unless they intentionally change the configuration of the client software to disallow those downloads and browsing commands from others on the network.

39. Files located in a network user's shared directory are processed by the client software. As part of this processing, a SHA1 hash value is computed for each file in the user's shared directory. SHA1 or Secure Hash Algorithm Version 1 is a file encryption method which may be used to produce a unique digital signature of a file. It is computationally infeasible (2^{160}) to find two different files that produce the same SHA1 value. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99 percent that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

40. Some P2P networks use SHA1 values to improve network efficiency. Users may receive a selected file from numerous sources by accepting segments of the file from multiple peers and then reassembling the complete file on the local computer. The client program succeeds in reassembling the file from different sources only if all the segments came from exact copies of the same file. The network uses SHA1 values to ensure exact copies of the same file are used during this process. It is possible to compare the SHA1 signatures of files being shared on the

network to previously identified SHA1 signatures of any file, including child pornography, to determine if the contents of the two files are identical.

41. A P2P file transfer is assisted by reference to an IP address. The IP address identifies the location of the computer with which the address is associated, making it possible for data to be transferred between computers. IP addresses can also assist law enforcement in finding a particular computer on the Internet. Typically, an IP address will lead the law enforcement officer to a particular Internet service company, and that company can then identify the account that used the IP address to access the Internet on a given date and time.

42. By receiving either a file list or portions of a download from a specific IP address, the investigator can conclude that a computer connected to that particular IP address is using a P2P software application to receive, distribute, and/or possess specific and known visual depictions of child pornography.

43. Even though P2P networks link together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user. The software is designed only to allow file that have been selected to be downloaded. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

44. A person that includes child pornography files in his/her "shared" folder is making those child pornography files available for other network users to download. Therefore, the hosting of child pornography in this way constitutes the promotion and distribution of child pornography in violation of federal law.

45. This investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of the officers involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in many seizures of child pornography and arrests for possession and distribution.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

46. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computers and computer-related media, to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, CDs, and USB thumb drives) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on-site or even within the period specified for execution of the search warrant.
- b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computers and computer-related media available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is ideal for a complete and accurate analysis.

47. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present

on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that they were created, as well as the sequence in which they were created. For example, by reviewing the Index.dat file (a system file that keeps track of historical activity conducted in the Internet Explorer application), it can be determined whether a user accessed other information close in time to the file creation dates, times and sequences so as to establish user identity and exclude others from computer usage during times related to the criminal activity.

48. I also know through the communication with digital forensic experts that the process of analyzing mobile devices takes on many forms. Many times the analysis of a mobile device can be completed by connecting the device to forensic applications, which will gather the data contained within that device. Although this is the first and primary means of analyzing mobile devices, there are instances where utilizing this non-destructive means is impossible. If a mobile device is protected by a password (that is not supplied by the suspect or a password that cannot be bypassed by forensic applications) it may still be possible to retrieve data. It may also be possible to extract data from phones that are designed to not connect with computers or forensic applications (TracFones). There are three current processes, which have been described to me by forensic experts. First, by utilizing a username and password to access a backup of the device stored on the cloud. Second, by removing the circuit board from the phone and soldering to points used by manufactures. These points allow direct access to the memory on the phone. This process may cause damage to the phone, but typically, the phone will remain intact and functional when

put back together. The last method is by removing the flash memory chip on the phone that actually stores the data on the phone. Once the chip is removed, forensic experts can read the data directly from the chip. This process will result in the permanent destruction of the phone; however, it allows for access to the data that was located on the phone. It is my training and experience that each of the methods described above for extraction will result in an accurate representation of some or all of the available data from the mobile device itself.

PROBABLE CAUSE

49. On May 17, 2018, Special Agent Senior Robert J. Thompson, conducted an authorized undercover Peer-to-Peer investigation. During this investigation; SAS Thompson located an internet protocol (IP) address of **75.120.112.180**, having possible child pornography available for download.

50. On May 17, 2018, SAS Thompson was able to connect, at 3:33 AM CST to the target IP address of **75.120.112.180**, and downloaded two (2) video files of suspected child pornography.

51. SAS Thompson reviewed the files of interest available for download from the target IP address of **75.120.112.180**, and noted, at the time of the downloads, that there were a total of two-hundred thirty-nine (239) files of interest that were available for download. For example, two (2) videos Agent Thompson downloaded, depicted females appearing to be twelve (12) years of age performing oral sex on an adult male. Based on this officer's training and experience, these two (2) file names were indicative of child pornography.

52. On May 17, 2018, I conducted an internet search to locate the internet service provider for the target IP address of **75.120.112.180** and was able to identify the provider as being CenturyLink.

Purdin-1823000001CE

53. On May 17, 2018, a subpoena was issued to CenturyLink for account information for IP address 75.120.112.180.

54. On May 17, 2018, I received a response from CenturyLink with the following account information:

Name: Robert Purdin

Address: 24988 Harmony Church Road, Andalusia, Alabama 36420

Account Number: 408585862

Home Phone: 334-427-3023

Secondary Contact: Tracy Purdin

Active Since: August 24, 2009

Research though numerous law enforcement databanks resulted in locating a person of interest, a Robert Purdin, W/M, DOB **/**/60, SSN ***-**-0674, and Tracy Purdin, W/M, DOB **/**/70, SSN ***-**-5470, residing at 24988 Harmony Church Road, Andalusia, Alabama 36420. Further information identifies Tracy Purdin as a registered sex offender.

55. Based on this officer's training and experience, individuals frequently carry and maintain cellular phones on their person. Also, digital storage media is often small enough to be concealed on one's person. Accordingly, this search warrant requests to search the person of any individual located at the SUBJECT PREMISES to locate such devices and digital storage media.

INFORMATION BASED UPON TRAINING AND EXPERIENCE

56. Based upon my training and experience, I know the following to be true:

- a. Those who have possessed and/or disseminated child pornography usually have an interest or preference in the sexual activity of children. Those who have demonstrated an interest or preference in sexual activity with children or in sexually explicit visual images depicting children are likely to keep

secreted, but readily at hand, sexually explicit visual images depicting children. In some instances, these depictions are actual photographs or images of the suspect's own sexual activity with past or present children. In some instances, the suspect keeps these depictions as a means of plying, broaching, or titillating the sexual interests of new child victims or otherwise lowering the inhibitions of other potential child sexual partners by showing them that other children participate in this kind of activity. Still, in other instances, the depictions are a means of arousing the suspect. These depictions tend to be extremely important to such individuals and are likely to remain in the possession of or under the control of such an individual for extensive time periods. Although he might, a person who has this type of material is not likely to destroy the collection. These sexually explicit visual images depicting children can be in the form of, but are not limited to, negatives, slides, books, magazines, videotapes, photographs or other similar visual reproduction, and digital image or video files.

- b. Persons trading in, receiving, distributing or possessing images or movies of child pornography often have copies of those files on their computer's hard drive or computer-related media. Even if the files were deleted by a user, they still may be recoverable by a trained computer forensic examiner.
- c. Persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child exploitation.
- d. Non-pornographic, seemingly innocuous images of minors are often found on media containing child pornography. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.
- e. Files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files.
- f. Computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of internet service accounts used to access the internet.

Purdin-1823000001CE

- g. Search warrants of residences involved in computer-related criminal activity usually produce items that would tend to establish ownership or use of computers and ownership or use of any internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.
- h. Search warrants of residences usually reveal items that would tend to show dominion and control of the property searched, to include utility bills, phone bills, correspondence, rental agreements and other identification documents.
- i. Based on my training and experience, because the individual using the IP address was sharing child pornography through P2P, the individual exhibits the characteristics of a person with a sexual interest in children and child pornography collector.

REQUEST FOR SEALING

57. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

CONCLUSION

Based upon the above, there is probable cause to believe that there is now concealed on the property located at 24988 Harmony Church Road, Andalusia, Alabama 36420 (see **Attachment A**) certain items as described in **Attachment B** that constitute instrumentalities and evidence of

Purdin-1823000001CE

the commission of a criminal offense, or are contraband, in violation of Title 18, United States Code, Sections 2252 and 2252A.

I respectfully request that the Court issue a warrant authorizing the search and seizure of 24988 Harmony Church Road, Andalusia, Alabama 36420, more fully described in **Attachment A**, and a further a seizure and search for those items listed in **Attachment B**. Said Attachments will be attached to the warrant.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Robert J. Thompson', written over a horizontal line.

Robert J. Thompson
Special Agent Senior, Alabama Bureau of Investigation
Task Force Officer, Department of Homeland Security

Subscribed to and sworn before me
this 30th day of May, 2018.

A handwritten signature in black ink, appearing to read 'Wallace Capel, Jr.', written over a horizontal line.
WALLACE CAPEL, JR.
CHIEF, UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

The residence, outbuildings, vehicles, curtilage, and persons located 24988 Harmony Church Road, Andalusia, Alabama 36420, is described in Covington County Tax records as a Mobile Home 48 x 32 built in 2007. Due to the location of the property, a more detailed description is not possible.



ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEIZED

The following items to be seized constitute contraband, fruits, instrumentalities, and evidence of crimes to wit: violations of Title 18, U.S.C. §§ 2252 and 2252A relating to the distribution, receipt, and possession of visual depictions of minors engaging in sexually explicit conduct and child pornography:

1. Any and all computers and computer-related media, as defined herein.
2. Any and all records, documents, and materials pertaining to any visual depiction of a minor engaging in sexually explicit conduct, child pornography, child erotica, a sexual interest in children, or sexual activity involving children.
3. Any and all records, documents, and materials pertaining to any minor who is, or appears to be, the subject of any visual depiction of a minor engaging in sexually explicit conduct, child pornography, child erotica, a sexual interest in children, or sexual activity involving children.
4. Any and all records, documents, and materials evidencing possession, use, or ownership of any of the premises to be searched or property to be seized.
5. Any and all records, documents, and materials that concern any internet accounts or any internet-related activity.
6. Any and all software that may be utilized to create, receive, distribute, store, modify, conceal, or destroy any of the evidence sought.

In the execution of this warrant, the agents may seize all computers and computer-related media to be searched later by a qualified examiner in a laboratory or other controlled environment.